KARTIKEYA SHARMA

Seattle, WA | (458) 250-9472 | kartikeya2015@gmail.com | linkedin.com/in/kart1 | github.com/kartikeyas00 | kartsec.dev

SUMMARY

Security and applied-ML engineer with 5+ years of experience building threat-detection, anomaly-detection, and analyst-automation systems. Specialized in graph neural networks, adversarial ML, and LLM-backed security workflows across endpoint, threat-intelligence, and firewall telemetry.

EXPERIENCE

Senior Associate Information Security Engineer - ML & Analytics | Equinix, Inc. | Jul 2023 – Present

- Designed and built a graph neural network pipeline for retrospective DDoS detection from millions of raw edge firewall events, modeling traffic as flow/host graphs across flow-based GNNs, heterogeneous Graph U-Nets, and unsupervised encoder-decoders.
- Developed an unsupervised anomaly-detection system over endpoint application-install data from CrowdStrike and Tenable, using K-Means clustering and cosine similarity to surface anomalous software across thousands of endpoints beyond standard EDR rules.
- Delivered a semantic string-matching service with embedding-backed matching and background processing for large files, reducing a recurring reconciliation workflow from multiple days to under an hour while preserving human verification.
- Built a bulk IOC enrichment tool aggregating multiple threat-intelligence sources into one analyst view, scaling investigations from manual one-at-a-time lookups to thousands of indicators per run.

Data Scientist | Veada Industries (Lippert Components) | Jul 2019 - Sep 2021

- Built and deployed a Flask/jQuery/REST project-management web app on AWS Elastic Beanstalk, replacing legacy software and manual processes and cutting manufacturing lead time by 50%.
- Trained a Scikit-learn/NLTK classifier to auto-categorize incoming orders, supporting labor- and material-planning decisions.
- Built internal Flask tools (electronic signature, vinyl patterning) that replaced paid commercial software and reduced software spend.

SELECTED SECURITY TALKS & PUBLICATIONS

- SaintCon 2025 - Adversarial Techniques for Bypassing GNN-Based Network Defense - Talk
- PNSQC 2025 - Graph Neural Network-Based DDoS Protection for Data Center Infrastructure - Paper
- BSides Austin 2024 - GPT as Ally: Improving Cybersecurity Workflows with GPT & Embedding APIs - Talk
- BSides Portland 2024 - Graphing the Insider: Innovative Applications of GNNs in Insider Threat Detection - Talk

EDUCATION

M.S. Computer Science, University of Oregon | 2021 - 2023 | GPA: 4.08
Relevant coursework: Machine Learning, Computer & Network Security, Distributed Systems, Multi-Agent Systems.

B.A. Computer Science & Accounting, Goshen College | 2015 - 2019

SERVICE

- **Judge**, Google I/O Hackathon 2026 (Cerebral Valley with Google DeepMind).
- **CFP reviewer** for BSides Red Rocks, BSides SLC, and BSides Cache; reviewed 300+ security talk submissions across multiple conferences.
- **Reviewer**, PNSQC 2025; reviewed research papers for technical quality, clarity, and venue fit.

SKILLS

Languages: Python, SQL, JavaScript, C/C++, Bash
ML & AI: PyTorch, DGL, Scikit-learn, pandas, NumPy, GNNs, anomaly detection, adversarial ML, LLM/agentic systems
Security & Cloud: Google Cloud, AWS, Elasticsearch, Google Chronicle SIEM/SOAR, CrowdStrike, Tenable, threat detection, IOC enrichment
Data: SQL Server, PostgreSQL, MySQL, Power BI